UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/726,841	12/02/2003	John Hines	127-0013	5556

22120 7590 03/01/2011

ZAGORIN O'BRIEN GRAHAM LLP
7600B NORTH CAPITAL OF TEXAS HIGHWAY
SUITE 350
AUSTIN, TX 78731

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
03/01/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/726,841	HINES ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 December 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims **3 - 23** are pending. Claim **16, 21** has been amended. Claims **1, 2** have been cancelled. Claims **3, 11, 16, 21** are independent. This application was filed 12-2-2003.

2. This action is in response to application amendments filed on 12-13-2010.

Response to Arguments

3. Applicant's arguments have been fully considered and were persuasive and new grounds of rejection have been entered.

3.1 The 101 Rejection for Claims 21, 22 is withdrawn due to the addition of the term non-transitory to computer readable medium. The 101 Rejection for Claim 16 - 18 is maintained due the lack of amendments to add a memory for the storage of instructions by the system. The specification on page 4 discloses an execution component that includes a data storage capacity but the claimed invention does not include a storage entity. The Specification Objection is maintained due to lack of amendments to add the term computer-readable medium to the specification.

3.2 Applicant argues, *a hash over a resultant state*.

Zhao discloses the processing of Certificate Revocation List (CRL) information using a delta or subset of CRL information instead of the entire set of CRL information. (see Zhao col. 5, lines 24-32: delta CRL is returned and processed by appending its

entries to current CRL (resultant state CRL)) CRL information processing using a partial or subset of the certificate revocation list is not novel and is disclosed by the current set of prior art consisting of Zhao and Bisbee.

Bisbee discloses the generation of a digital signature consisting of a hash using a delta CRL or an entire CRL. A delta CRL is a resultant state of a CRL. Bisbee discloses the generation of a hash using a resultant state (delta CRL). (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash) And, Bisbee discloses a comparison of hash values for verification purposes. (see Bisbee paragraph [0008], lines 5-9: resultant first hash (created from decryption of previously encrypted hash) compared to re-hash of second hash of original information object)

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: **Claims 21, 22** are objected as "**computer readable encoding**" is not defined clearly in the specification, so that the meaning of the term in the claims is not ascertainable by reference to the specification.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims **16 - 18** are rejected under 35 USC 101 since the claims are directed to non-statutory subject matter.

Claims **16 - 18** are to be construed as a computer system of *"software per se"*, unless the specification makes clear the only reasonable interpretation of the word *" system"* includes at least one tangible hardware inclusive component. The specification is silent as to any definition for a system. In the broadest sense, Claims **16 - 18** are directed towards non-statutory. Applicant must indicate at least one tangible hardware components such as a memory for storage of program instructions.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims **3 - 23** are rejected under 35 U.S.C. 103 (a) as being unpatentable over **Zhao et al.** (US Patent No. **7,124,295**) in view of **Bisbee et al.** (US PGPUB No. **20040093493**).

With Regards to Claim 3, Zhao discloses a method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:

b) computing an update to a local certificate revocation list state by applying the received delta CRL to produce a resultant local CRL state; (see Zhao col. 5, lines 24-32: delta CRL is returned and processed by appending its entries to current CRL (resultant state CRL))

Zhao discloses receiving a delta coded update to a certificate revocation list (a delta CRL) together with an associated first hash value, the delta CRL encoding an update to a preceding certificate revocation list state CRL(t). (see Zhao col. 3, lines 5-10: CRL spanning from most recent CRL to the current CRL; updated delta CRL)

Zhao does not specifically disclose first hash value computed as a function of a resultant state CRL(t+1) and a second hash value as a function of resultant local CRL state.

However, Bisbee discloses:

a) receiving an associated first hash value, the first hash value computed as a function of at least a resultant state CRL(t+n) computable by applying the delta CRL to the CRL(t) state; c) by computing a second hash value as a function of at least the resultant local CRL state; (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since

last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

A delta CRL is a temporal (time-based) generated data structure. A delta CRL is a certificate revocation list for PKI certificates revoked from a first time (t1) to a second time (t2). Bisbee discloses the generation and usage of the delta CRL data structure. In addition, Bisbee discloses the generation of a hash value as part of the generation of a digital signature when a delta CRL is signed.

Zhao does not specifically disclose comparing second and first hash values. However, Bisbee discloses:

c) validating the update at least in part by comparing the second and first hash values. (see Bisbee paragraph [0008], lines 5-9: resultant first hash (created from decryption of previously encrypted hash) compared to re-hash of second hash of original information object)

It would have been obvious to one of ordinary skill in the art to modify Zhao for first hash value computed as a function of a resultant state CRL(t+1) and a second hash value as a function of resultant local CRL state, and comparing second and first hash values as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits achieved from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 4, Zhao discloses the method of claim 3, further comprising: requiring, as a condition precedent to the update, that a transmission that conveys the delta CRL include a valid digital signature establishing a trusted source thereof. (see Zhao col. 5, lines 39-41: signature attached to delta CRL)

With Regards to Claim 5, Zhao discloses the method of claim 3. (see Zhao col. 3, lines 5-10: delta CRL processing system)

Zhao does not specifically disclose first hash value computed as a function of both the CRL(t) and CRL(t+1) states and second hash value computed as a function of both a prior local CRL state and the resultant local CRL state.
However, Bisbee discloses wherein the first hash value is computed as a function of both the CRL(t) and CRL(t+1) states, and wherein the second hash value is computed as a function of both a prior local CRL state and the resultant local CRL state. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of a hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for first hash value computed as a function of both the CRL(t) and CRL(t+1) states and second hash value computed as a function of both a prior local CRL state and the resultant local CRL state as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope

of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 6, Zhao discloses the method of claim 3, further comprising: requesting a CRL update, the request indicating a base t beyond which update is desired; and receiving in response to the request, plural delta CRLs including the first delta CRL and at least one other delta CRL together. (see Zhao col. 3, lines 5-10: request/response for update CRL; Figure 4; col. 5, lines 4-9: multiple delta CRLs)

Zhao does not specifically disclose each hash value computed as a function of a respective resultant certificate revocation list (CRL) state.
However, Bisbee discloses respective associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of a respective resultant certificate revocation list (CRL) state. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for each hash value computed as a function of a respective resultant certificate revocation list (CRL) state as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI

systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 7, Zhao discloses the method of claim 6. (see Zhao col. 3, lines 5-10: delta CRL generation system)

Zhao does not specifically disclose each hash value computed as a function of both a respective prior CRL state and respective resultant CRL state.
However, Bisbee discloses wherein each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for each hash value computed as a function of both a respective prior CRL state and respective resultant CRL state as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 8, Zhao discloses the method of claim 6, further comprising: performing successive updates to the local certificate revocation list state by applying successive ones of the delta CRLs received in response to the request; and validating

the successive updates based on the respective associated hash values. (see Zhao col. 5, lines 4-9: multiple deltas CRLs)

With Regards to Claim 9, Zhao discloses the method of claim 6, wherein the base t is a temporal index. (see Zhao col. 1, lines 17-19: is a time index for certificate revocation)

With Regards to Claim 10, Zhao discloses the method of claim 3, further comprising: if the validating is unsuccessful, requesting a complete copy of a current certificate revocation list. (see Zhao col. 5, lines 27-30: transfer complete copy of CRL (updates appended to previous CRL, entire CRL)

With Regards to Claim 11, Zhao discloses a method for coordinating update of certificate revocation information in a distributed public key infrastructure (PKI) environment, the method comprising:

a) preparing a first delta coded update to a certificate revocation list (a first delta CRL), the first delta CRL encoding an update sufficient to produce a subsequent certificate revocation list state CRL(t+1) from a preceding certificate revocation list state CRL(t); (see Zhao col. 3, lines 5-10: updated information (delta CRL) for CRL (first, second)

Zhao discloses transmitting the delta CRL, and a base t. (see Zhao col. 3, lines 5-10: delta CRL transmitted in reply to request; col. 1, lines 17-19: base t (temporal)

processing for delta information)

Zhao does not specifically disclose computing an associated first hash value as a function of CRL(t+1) state.

However, Bisbee discloses:

b) computing an associated first hash value as a function of at least the CRL(t+n) state; (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

Zhao discloses transmitting the associated value in response to a request for certificate revocation list update beyond a base t. (see Zhao col. 3, lines 5-10: delta CRL transmitted in reply to request; col. 1, lines 17-19: base t (temporal) processing for delta information)

Zhao does not specifically disclose the associated hash value.

However, Bisbee discloses:

c) the associated first hash value; (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for

computing an associated first hash value as a function of CRL(t+1) state and the associated first hash value as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 12, Zhao discloses the method of claim 11. (see Zhao col. 3, lines 5-10: delta CRL processing system)

Zhao does not specifically disclose first hash value is computed as a function of both the CRL(t) and CRL(t+n) states.
However, Bisbee discloses wherein the first hash value is computed as a function of both the CRL(t) and CRL(t+1) states. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for first hash value computed as a function of both the CRL(t) and CRL(t+n) states as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 13, Zhao discloses the method of claim 11, further comprising: receiving a CRL update request indicating a base t beyond which update is desired; and transmitting in response to the request, plural delta CRLs including the first delta CRL and at least one other delta CRL together with respective. (see Zhao col. 3, lines 5-10: delta CRL request/response; col. 1, lines 17-19: base t (time index) processing; col. 5, lines 4-9: multiple delta CRLs)

Zhao does not specifically disclose each hash value computed as a function of a respective resultant certificate revocation list (CRL).
However, Bisbee discloses associated hash values including the first hash value and at least one other hash value, wherein each hash value is computed as a function of at least a respective resultant certificate revocation list (CRL) state from which the associated delta CRL is derived. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for each hash value computed as a function of a respective resultant certificate revocation list (CRL) as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 14, Zhao discloses the method of claim 13. (see Zhao col. 3, lines 5-10: delta CRL processing system)

Zhao does not specifically disclose each hash value computed as a function of both a respective prior CRL state and respective resultant CRL state.
However, Bisbee discloses wherein each of the hash values is computed as a function of both a respective prior CRL state and the respective resultant CRL state from which the associated delta CRL is derived. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for each hash value computed as a function of both a respective prior CRL state and respective resultant CRL state as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 15, Zhao discloses the method of claim 13, further comprising:

a) performing successive updates to the local certificate revocation list state by applying successive ones of the delta CRLs received in response to the request; (see Zhao col. 5, lines 4-9: update CRL information with multiple delta CRLs)

Zhao does not specifically disclose validating successive updates based on comparison of associated hash values.

However, Bisbee discloses:

b) validating the successive updates based on comparison of the associated hash values with respective locally computed hash values; (see Bisbee paragraph [0008], lines 5-9: resultant first hash (created from decryption of previously encrypted hash) compared to re-hash of second hash of original information object)

It would have been obvious to one of ordinary skill in the art to modify Zhao for validating successive updates based on comparison of associated hash values as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 16, Zhao discloses a system at least partially implemented in hardware and comprising:

a) first and second validation authorities (VAs) communicatively coupled to propagate certificate revocation list (CRL) information; (see Zhao col. 2, lines 44-46: certification authority (validation authorities))

Zhao discloses the first VA configured to prepare delta CRLs in correspondence with updates from a certificate authority (CA), each delta CRL encoding a respective

update sufficient to produce a next certificate revocation list state CRL(t+1) from a preceding certificate revocation list state CRL(t); (see Zhao col. 2, lines 44-46: multiple Certificates Authorities (VAs); col. 3, lines 5-10: generate a delta CRL based on a request)

Zhao discloses the second VA configured to receive the delta CRLs from the first VA, to calculate based thereon updates to local certificate revocation list states by applying the received delta CRL to produce a resultant local CRL state. (see Zhao col. 2, lines 44-46: multiple Certificate Authorities (CAs); col. 2, lines 57-62: apply delta CRL to produce resultant CRL)

Zhao does not specifically disclose to compute first hash values as a function of respective sequentially adjacent pairs of states CRL(t) and CRL(t+1), and comparison of respective first hash values with second hash values.

However, Bisbee discloses:

b) wherein further configured to compute respective first hash values as a function of respective sequentially adjacent pairs of states CRL(t) and CRL(t+1) and a hash received from a VA, and computed as a function of respective prior local CRL states and resultant local CRL states. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

c) wherein to validate each update based at least in part on comparison of

respective first hash values with second hash values; (see Bisbee paragraph [0008], lines 5-9: resultant first hash (created from decryption of previously encrypted hash) compared to re-hash of second hash of original information object)

It would have been obvious to one of ordinary skill in the art to modify Zhao to compute first hash values as a function of respective sequentially adjacent pairs of states CRL(t) and CRL(t+1), and comparison of respective first hash values with second hash values as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 17, Zhao discloses the system of claim 16, wherein transmission of a given delta CRL. (see Zhao col. 5, lines 39-41: digital signature utilized for security)

Zhao does not specifically disclose a first hash value.
However, Bisbee discloses its associated first hash values are secured using a digital signature. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for a first hash value as taught by Bisbee. One of ordinary skill in the art would have been

motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 18, Zhao discloses the system of claim 16, wherein the delta CRLs and associated first hash values are received via an intermediary. (see Zhao col. 5, lines 24-27: remote server (intermediary) received delta CRLs)

Zhao does not specifically disclose a first hash value.
However, Bisbee discloses wherein first hash values. (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for a first hash value as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 19, Zhao discloses a computer program product encoded in one or more media and including instruction sequences executable on a processor of a system that hosts a validation authority to perform the receiving, computing and validating steps of claim 3. (see Zhao col. 6, lines 33-41: software implementation,

instructions)

With Regards to Claim 20, Zhao discloses a computer program product encoded in one or more media and including instructions sequences executable on a processor of a system that hosts a validation authority to perform the preparing, computing and transmitting steps of claim 10. (see Zhao col. 6, lines 33-41: software implementation, instructions)

With Regards to Claim 21, Zhao discloses a non-transitory computer readable medium encoding comprising:

a) delta coded certificate revocation list (CRL) update data that allows a receiving validation authority to generate an updated CRL by applying the delta coded CRL update to a previous CRL state; (see Zhao col. 3, lines 5-10: generate a delta CRL list)

c) a digital signature establishing identity of a source of the computer readable encoding. (see Zhao col. 5, lines 39-41: digital signature appended)

Zhao does not specifically disclose hash computed as a function of the next certificate revocation list state CRL(t+n) by applying the delta coded CRL update to a previous certificate revocation list state CRL(t).

However, Bisbee discloses:

b) a self-validating indicator encoded in association with the delta coded CRL update, the self-validating indicator encoding a hash computed not as a function

of the delta coded CRL update itself, but rather as a function of the next certificate revocation list state CRL(t+1) which may be generating by applying the delta coded CRL update to a previous certificate revocation list state CRL(t); (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for hash computed as a function of the next certificate revocation list state CRL(t+n) by applying the delta coded CRL update to a previous certificate revocation list state CRL(t) as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 22, Zhao discloses the computer readable medium of claim 21. (see Zhao col. 3, lines 5-10: delta CRL information processing system)

Zhao does not specifically disclose hash is computed as a function of both the next state CRL(t+1) and the previous state CRL(t).
However, Bisbee discloses wherein the encoded hash is computed as a function of both the next state CRL(t+n) and the previous state CRL(t). (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring

since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for a hash is computed as a function of both the next state CRL(t+1) and the previous state CRL(t) as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

With Regards to Claim 23, Zhao discloses the method of claim 3, further comprising:

a) preparing the delta coded update to the certificate revocation list, the delta CRL encoding an update sufficient to produce the resultant state CRL(t+1) from the preceding certificate revocation list state CRL(t); (see Zhao col. 3, lines 5-10: CRL spanning from most recent CRL to the current CRL; updated delta CRL)

Zhao does not specifically disclose computing the associated first hash value as a function of at least the resultant state CRL.

However, Bisbee discloses:

b) computing the associated first hash value as a function of at least the resultant state CRL(t+1); (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0072], lines 5-8: every (including delta CRL) is signed; paragraph [0008], lines 5-9: create a digital signature by generation of hash)

Zhao discloses for c): transmitting the delta CRL and the associated first hash value in response to a request for certificate revocation list update beyond a base t. (see Zhao col. 3, lines 5-10: delta CRL transmitted in reply to request; col. 1, lines 17-19: base t (temporal) processing for delta information)

Zhao does not specifically disclose a first hash value.

However, Bisbee discloses:

c) the associated first hash value (see Bisbee paragraph [0034], lines 1-11: process status as a delta certificate revocation list (only changes occurring since last publication); paragraph [0008], lines 5-9: create digital signature by generation of hash)

It would have been obvious to one of ordinary skill in the art to modify Zhao for computing the associated first hash value as a function of at least the resultant state CRL(t+1) and a first hash value as taught by Bisbee. One of ordinary skill in the art would have been motivated to employ the teachings of Bisbee for the benefits from expanding the scope of operational CA and PKI systems by enabling interoperability with any CA and PKI systems. (see Bisbee paragraph [0029], lines 3-8)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
February 14, 2011

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436